AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2000 Smith Road
Hamilton, OH 45013

Case No. 1:14MJ -634

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Ohio
(identify the person or describe the property to be searched and give its location):

2000 Smith Road, Hamilton, OH 45013. Also, see Affidavit and Attachments.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Affidavit and Attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 10/29/14
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Karen L. Litkovitz.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 10/15/14@1:45pm Karen L. Litkovitz
Judge's signature

City and state: Cincinnati, OH Karen L. Litkovitz, United States Magistrate Judge
Printed name and title

GOVERNMENT EXHIBIT 2

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

14 OCT 15 PM 1:49

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2000 Smith Road
Hamilton, OH 45013

Case No. 1:14MJ -634

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

2000 Smith Road, Hamilton, OH 45013. Also, see Affidavit and Attachments.

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Affidavit and Attachments.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(g); 2251 (d)(1)&(e); 2252A(a)(2)(A)&(b)(1); 2252A(a)(5)(B)&(b)(2)	Engaging in child exploitation enterprise; advertising, etc. re child pornography; receipt/distribution of child pornography; knowing access/attempt with intent to view child pornography.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT AND ATTACHMENTS.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pamela S Kirschner
Applicant's signature

Special Agent Pamela S. Kirschner, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/15/14

Karen L. Litkovitz
Judge's signature

City and state: Cincinnati, OH

Karen L. Litkovitz, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

14 OCT 15 PM 1:49

IN THE MATTER OF THE SEARCH OF:	)	
2000 Smith Road	)	**UNDER SEAL**
Hamilton, Ohio 45013	)	Case No.
	)	1:14MJ -634

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

INTRODUCTION

I, Pamela S. Kirschner, being duly sworn, hereby depose and state as follows:

1. I have been employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) since 1997, and am currently assigned to the Cincinnati Office of the FBI. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I have probable cause to believe that evidence of a crime, fruits of a crime, contraband and instrumentalities of violations of: 18 U.S.C. § 2252A(g) (engaging in a child exploitation enterprise); 18 U.S.C. § 2251(d)(1) and (e), (advertising, attempting to advertise, and conspiracy to advertise child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute

child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (knowing access, conspiracy to access, or attempted access with intent to view child pornography) are located within the residence at 2000 Smith Road, Hamilton, Ohio 45013, and any adjacent outbuildings, (hereinafter the "SUBJECT PREMISES"). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachments A and B, incorporated herein by reference, which is located in the Southern District of Ohio. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing advertising, production, transportation, shipment, receipt, possession, distribution, access with intent to view, and reproduction of child pornography, as well as the attempt and conspiracy to violate the foregoing. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling, any outbuildings, and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

4. The statements contained in this affidavit are based in part on: information provided by FBI SAs; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies as described below; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as an SA with the FBI. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

5. The instant investigation, described more fully below, involves an Internet-based website referred to as "Website 19".[1] The instant investigation has revealed that an individual residing at the SUBJECT PREMISES was a registered member of "Website 19" who uploaded child pornography to "Website 19."

RELEVANT STATUTES

6. This investigation concerns alleged violations of: 18 U.S.C. § 2252A(g) (engaging in a child exploitation enterprise); 18 U.S.C. § 2251(d)(1) and (e), (advertising, attempting to advertise, and conspiracy to advertise child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (knowing access, conspiracy to access, or attempted access with intent to view child pornography);

a. 18 U.S.C. § 2252A(g) prohibits any person from violating Chapter 110 of Title 18 of the United States Code, as a part of a series of felony violations constituting three or more separate incidents and involving more than one minor victim, where those offenses are committed in concert with three or more other persons.

b. 18 U.S.C. § 2251(d)(1) and (e) prohibits a person from knowingly making, printing or publishing, or causing to be made, printed or published, or attempting or conspiring to make, print or publish, any notice or

---

1

[1] The particular website described in this affidavit has been referred to in other legal process by the number used in this affidavit, so this number is being used here for consistency. The actual name of the website is known to law enforcement. Investigation into the users of this site remains ongoing and disclosure of the name of the site would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

c. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

d. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

7. The following definitions apply to this Affidavit:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread" refers to a linked series of posts and reply messages. Message threads often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the bulletin board administrator.

b. "Child erotica," as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

c. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the

visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A DNS (domain name system) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or

transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of

digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

k. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically

charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

m. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

n. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies),

mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

q. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

s. Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides privacy and authentication for data communication

such as text, e-mails, and files.

PROBABLE CAUSE

8. A user of the Internet account at SUBJECT PREMISES has been linked to "Website 19," a website whose primary purpose is to advertise and distribute child pornography. There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES became a registered member of "Website 19" and uploaded child pornography to "Website 19."

Description of "Website 19"

9. "Website 19" is an active online bulletin board whose primary purpose is the advertisement and distribution of child pornography. As of September 24, 2014, statistics posted on "Website 19" reveal that the board contains a total of 368,220 posts, 90,635 total threads, and 45,403 total members. "Website 19" requires its users to continually share child pornography in order to gain and keep membership.

10. "Website 19" is organized by different topical areas or forums. For example, "Application Rules" or "Hardcore" would have individual threads containing posts that one would expect to topically conform to the forum heading. A review of the initial forums accessible on "Website 19" prior to registering an account with the website revealed a post entitled "Application Rules," which contained the following instructions, among other things:

a. …Must contain clearly preteen hardcore material (does NOT need to be private, rare or new); no softcore, no JB or borderline JB; if at least one of the participants is 12 years old or less, flat-chested, hairless and engaging in sexual activity, it most likely qualifies (this requirement applies to applications only)….

b. …Must have 50-200 MB of total uploads, which may consist of one or more videos or imagesets in a single post; posts containing less than 50 or more than 200 MB of uploads will be rejected (this requirement applies to

applications only)....

c. ...An Admin Team member will review your application post and, if not approved, a reply will be posted that explains what is missing or incorrect with the post. Please allow up to 48 hours for the review process to be completed. Once you have created a post that conforms to the rules, you will be promoted to Full Member and be granted access to the posting forums.

11. Another forum on "Website 19" that was available prior to registering an account contained a post entitled "Activity Rules and Posting Information." Review of this post revealed the following text, among other things:

a. ... What does count as a contribution and what does not? COUNT as contribution:
Set(s) of pictures and/or videos displaying child/teen (pubescent) modeling, child/teen (pubescent) nudity, softcore or hardcore erotica.
Nudism/naturism.
Webcam captures.
Working *backdoors* and passwords of on-topic sites (if they don't require JavaScript or Flash).
Helping the community with tutorials, re-uploads and filling requests of all of the above.....

b. ...DON'T COUNT as contribution:
Late teen nudity/erotica/porn (Jailbait who passed puberty and look like adults: ±14 years old for girls and ±15 years old for boys).
Adult nudity/erotica/porn. This includes fake jailbait porn (young looking women that act like teenagers but are obviously 18+)

c. All Full Members are required to contribute at least once every 30 days. The first 30-day contribution period begins on the day of promotion to Full Member.

d. VIP Members: All VIP Members are required to contribute at least once every 30 days, in any section of the board.

e. SVIP Members: All SVIP Members are required to contribute at least once every 30 days, in any section of the board.

12. After reviewing the above forums and postings, on July 23, 2014, an undercover FBI agent then accessed "Website 19" using an account previously registered on the website by a

user of the website and subsequently seized by law enforcement pursuant to the user's consent to assume his online identity.

13. After successfully logging into "Website 19", a review of the various topics within the forums (such as "Hardcore," "Pics," and "Vids") revealed, among other things, numerous image and/or video files that contained child pornography or child erotica. The images included depictions of prepubescent females, males, and toddlers with their genitals lasciviously exhibited[2], as well as the same prepubescent females, males, and toddlers engaged in sexual acts. The sexual acts included anal, vaginal, or oral penetration. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail previews of images, compressed files (such as ".rar" files), links to external sites, or replies to previous posts.

14. Examples and descriptions of posts containing child pornography depicting prepubescent females and males are as follows:

a. On July 23, 2014, a user posted a topic in the Webcams-Boys forum that contained numerous images depicting child pornography and child erotica of prepubescent males. Several of these images depicted the naked prepubescent males lying next to each other with their legs spread apart, exposing their genitalia, and holding their penises.

b. On July 11, 2014, a user posted a topic in the Hardcore-Girls-Pics forum that contained numerous images depicting child pornography and child erotica of a prepubescent female. Several of these images depicted the naked prepubescent female lying on what appeared to be a bed with her legs spread

---

2 In each of these depictions, the minors were nude or partially nude with their genitals clearly exhibited in the depiction. The genitals were the focal point of the image and the minors were posed in a sexual way to clearly elicit a sexual response in the viewer.

apart and being anally and vaginally penetrated by an adult male.

15. A private message feature was also available on the site that allowed users to send each other private messages.

Finding and Accessing "Website 19"

16. "Website 19" operates on a computer network, hereinafter "the Network," available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. In order to access that Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the network's administrators, or downloading a publicly-available third-party application.[3] Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

17. Websites that are accessible only to users within the Network can also be set up within the Network. "Website 19" is just such a website. A user could only reach websites like "Website 19" if the user is operating in the Network. Even after connecting to the Network, however, a user must have known the exact web address of such a website in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not have simply performed a Google search for the name of "Website 19" to obtain the web address for "Website 19" and click on a link to navigate to "Website 19." Rather, a user might have obtained the web address for

---

3 Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the anonymizing benefits of the Network.

"Website 19" directly from other users of "Websites 19," or from online postings describing both the sort of content available on "Website 19" and its location. Accessing "Website 19" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website 19" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

The Instant Messaging Service

18. The Instant Messaging Service (hereinafter "IMS")[4] is a free, publically available instant messaging service that allows Network users to send instant text messages and files to one another. Users may install the IMS on their computer and then obtain a unique IMS username to be able to communicate with other IMS users.

19. The unique IMS username is a pseudo-random string of characters created by the IMS, via a particular algorithm, when the software is downloaded and installed for the first time. The IMS username cannot be used from two different computers at the same time and because of the length of the username and the way it is generated, it is almost impossible that a unique IMS username would be recycled and given to a different user at another time.

User "argonaut" on Website 19"

20. While accessing "Website 19" in an undercover capacity using an account previously seized by law enforcement, an undercover FBI agent observed the user profile of "Website 19" user "argonaut." Profile information on "Website 19" may include contact information and other information that is supplied by the user. It also contains information about

---

4 The actual name of the Instant Messaging Service (IMS) is known to law enforcement. Investigation into criminal suspects who used the service remains ongoing and disclosure of the name of the service would potentially alert users to the fact that law enforcement is able, with appropriate legal process, to obtain information about accounts on the IMS, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts.

21. The profile page of user "argonaut" indicated this user originally registered an account on "Website 19" on April 23, 2013. According to this user's profile, as well as the member list maintained by "Website 19," the user "argonaut" is a Co-Administrator of "Website 19." The avatar picture associated with user "argonaut" is a photo of a nude pre-pubescent Caucasian male. According to the statistics on user "argonaut's" profile page, between April 23, 2013, and September 13, 2014, this user made a total of approximately 2,096 postings to "Website 19." Site data also indicates "argonaut" sent a total of approximately 1,183 private messages on "Website 19." During the same period, the user "argonaut" made 361 "contribution posts." "Contribution posts" refer to postings of images or videos. Examples of these postings are as follows:

22. On March 27, 2014, user "argonaut" posted a message titled "Sponge Bob" that contained preview images depicting a prepubescent male engaging in oral sex and masturbation with an adult male.

23. On May 17, 2014, user "argonaut" posted a message titled "Nino deli" that contained preview images depicting a prepubescent child with a shirt pulled up, exposing his penis, and the hand of an adult male manipulating that penis in actual or simulated masturbation.

24. On July 29, 2014, the user "argonaut" made a post to the thread titled VideoKidsBrazil01 and 02. The preview images in the thread contained 25 images, which contained child pornography; including those depicting naked prepubescent males engaging in sexual activity. The images depict prepubescent males engaging in or simulating masturbation. The user "argonaut" posted text to the thread that read, "this version is still screwed up but at

least you can seek around to get to the other stuff in the video."

25. On August 24, 2014, the user "argonaut" made a post to the thread BoyParty [7-10 yo]. The user "argonaut" posted text to the thread that read, "I stumbled across this file...looks like it's part 4 which goes with part 1 ((Boyparty) Mj 6Yo Boy (with Dad).mpg) above. does anyone have the missing pieces?" The contact sheet in the thread contained nine images, the majority of which contained child pornography; including images depicting a naked prepubescent male engaging in sexual acts including masturbation with an adult male.

26. All of the preceding postings followed site rules about posting preview images, external links to child pornography content and passwords to decrypt downloaded files.

27. Investigators also located numerous examples of user "argonaut" engaging in administrative activity on "Website 19." For instance, site records show that he deleted posts on August 31, August 20, July 29, July 20, 2014, among other dates. Site records also show that he edited posts on May 16, May 19, May 27, and September 10, 2014, among other dates.

28. On March 11, 2014, in response to a private message from another user inquiring about monthly posting requirements for "Website 19," the user "argonaut" responded (among other text): "...don't worry, demotions don't happen automatically, they are manually checked by admins. if we see a post like that which was approved then edited back to normal status when we're checking for demotions, we will make sure it counts and you don't get demoted."

29. On August 26, 2014, in response to a private message from another user inquiring about promotion to VIP status on "Website 19," the user "argonaut" responded: "i moved the new links to your old posts and deleted the new posts so everything is cleaned up. the anonfiles for daphne aren't working just now but i suppose that's a temporary problem. since you've gone ahead and fix all these problems i can promote you but I ask you fix your other flagged posts as

well. .zip to .rar. just edit the old posts with the new links. thanks."

30. On August 30, 2014, in response to a private message from another user of "Website 19," user "argonaut" responded: "aha. i've found being an admin is a ton of work. So much clerical work. If I wanted to be a cleric i would have joined the church, at least they have altar boys. seriously thou i don't want to give up my position. but i can see how you can get burned out with the job."

Evidence Related to Identification of user "argonaut"

31. In approximately June 2014, during the execution of a search warrant, foreign law enforcement seized the computer of an administrator of "Website 19." During a search of his computer, foreign law enforcement discovered a database backup from March of 2014 containing the content associated with "Website 19." In June of 2014, the foreign law enforcement provided a copy of that database to the FBI. In reviewing that data, a post was discovered dated September 29, 2014, by a "Website 19" administrator where he requested that all of the administrators list their IMS Usernames, by editing the posting themselves (which they could do because they have administrative rights on the site). User "argonaut" complied and listed an IMS Username in that posting.

32. In June of 2014, an Administrative subpoena was issued to an electronic communications service provider[5] who provided information that an individual utilizing the IMS Username listed by "argonaut" in that posting as of March 14, 2014 (the date of a backup copy of "Website 19" seized by foreign law enforcement) from IP address 24.209.235.71 on multiple

[5] The actual name of the electronic communications service provider is known to law enforcement. Investigation into criminal suspects who used the IMS remains ongoing and disclosure of the name of the communications service provider would potentially alert users to the fact that law enforcement is able, with appropriate legal process, to obtain information about IMS accounts, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

occasions, including February 24, 2014, April 22, 2014, and several dates and times in-between these two dates. In July of 2014, an Administrative subpoena was issued to Time Warner Cable in regards to IP address 24.209.235.71 on February 24, 2014 and April 22, 2014. A review of the results obtained identified the following account holder: Jason Gmoser, 2000 Smith Road, Hamilton, Ohio 45013. The internet service was started in January 2012.

33. A check of publicly available databases revealed a Jason T. Gmoser, born September 24, XXXX, Social Security Account Number 268-86-XXXX, resides at 2000 Smith Road, Hamilton, Ohio 45013. A check of the Ohio Bureau of Motor Vehicles revealed Jason T. Gmoser, Driver's License number RT152705, born on September 24, XXXX, SSAN 268-86-XXXX, resides at 2000 Smith Road, Hamilton, Ohio 45013.

34. On October 9, 2014, a physical surveillance was conducted of SUBJECT PREMISES, but the residence could not be seen from the road. There is a black metal entrance gate flanked by a semi-circle shaped stone and concrete wall façade with long decorative grasses. The driveway travels through a wooded area towards the house.

35. A review of map information from the Butler County's Auditor's Office identifies SUBJECT PREMISES as having a total of 5.8520 acres of land. The entrance façade described above is viewable in the land map for SUBJECT PREMISES. The residential dwelling is listed as a 1.5 story frame constructed building with approximately 3000 square feet of living space. A review of the photographs of the residence shows a contemporary A-frame designed structure with ample decking and a detached oversized two-car garage. In some pictures, the residence appears to have brown siding, and in others, it appears to be gray.

36. On October 11, 2014, further surveillance was conducted and revealed that in addition to the detached garage, there is also a hayloft-barn type of structure on the property with

some miscellaneous equipment located nearby.

37. It is your Affiant's experience that almost all homeowners currently use wireless routers to connect to various wireless devices in their homes. Furthermore, it appears that a wireless signal located in the residence would be reachable by a wireless device being used in any of SUBJECT PREMISES' outbuildings.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW AND/OR PRODUCE, RECEIVE, DISTRIBUTE, OR POSSESS CHILD PORNOGRAPHY

38. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view and/or produce, possess, receive, or distribute images of child pornography:

a. Individuals who access with intent to view and/or produce, possess, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who access with intent to view and/or produce, possess, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media.

Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who access with intent to view and/or produce, possess, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondences, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who access with intent to view and/or produce, possess, receive, or distribute pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who access with intent to view and/or produce, possess, receive, or distribute child pornography also may correspond with and/or meet

others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring child pornography images.

g. Individuals who access with intent to view and/or produce, possess, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Individuals who access with intent to view and/or produce, possess, receive, or distribute child pornography often use software to encrypt devices to conceal child pornography or similar material from law enforcement.

39. Based on the following, I believe that a user of the Internet account at SUBJECT PREMISES, likely displays characteristics common to individuals who access with intent to view and/or produce, possess, receive, or distribute child pornography. For example, the target

of investigation:

a. Became a user of "Website 19", whose primary purpose was to advertise and distribute child pornography;
b. Posted child pornography to "Website 19;"
c. Administered "Website 19."

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

40. Computers and digital technology have revolutionized the way in which individuals interested in child pornography interact with one another. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

41. The development of computers and digital cameras has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

42. Individuals who access with intent to view and/or possess, receive, distribute or advertise child pornography can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital

cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store over 100 gigabytes of data, which provide enough space to store thousands of high-resolution photographs. Video camcorders that once recorded video onto tapes or mini-CDs can now save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

43. A device known as a modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

44. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte (1000 gigabytes) external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small

devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them.)

45. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

46. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

47. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

48. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by

malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

49. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

50. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

51. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not

immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

52. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into a criminal organization, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal continuations and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, such as by posting them publicly online through forums. Premature disclosure of the contents of this continuation and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

REQUEST FOR AUTHORITY FOR NO-KNOCK WARRANT

53. On February 15, 2014, "argonaut" sent a private message to another user on "Website 19" which instructs that user on the proper use of TrueCrypt software. TrueCrypt is known to your affiant as a program that would allows a user to fully encrypt their computer and/or files on that computer.

54. Based upon the above information, there is a reasonable probability that the subject under investigation uses encryption software which, if activated, may prevent law enforcement from obtaining the information stored in the computers which are subject to seizure. If, at the time agents enter to execute this search warrant, an encrypted computer is powered off or locked, then the encryption would be activated and it would be difficult or impossible to search that device without the necessary password or pass-phrase. To avoid the scenario where

agents encounter an encrypted computer or computers, agents will attempt to execute this warrant at any time of day or evening when the subject under investigation is home and computers at the subject location are up and running and being used to send or receive data over the Internet. Precautions also need to be taken to ensure that the subject under investigation does not activate encryption when agents arrive at the home to serve the warrant. Activating that encryption can be as simple as pressing a button on a computer or powering a computer down, which takes a matter of seconds. If the subject under investigation or others in the premises is aware of the search prior to the actual entry of the agents who are conducting the search, the encryption software can therefore be easily activated.

55. This has proven to be true in the instant investigation. Prior search warrants obtained by the FBI and foreign law enforcement agencies have identified multiple subjects whose computers contained encryption software. In several of these instances, law enforcement was able to execute the warrants with court-authorized no-knock authority at times when the subjects were at home and the computers at these locations were up and running. This resulted in law enforcement obtaining information leading to multiple identifications and arrests of criminal suspects who were sexually abusing children, producing child pornography, and trafficking in child pornography. For example, during the execution of a search warrant on one user of "Website 19," the subject attempted to pull his power cables out of the wall to shut down his computer before law enforcement agents took him into custody. The subject did manage to pull a power cable but he missed and grabbed the wrong one. If he had pulled the proper cable his computer would have been shut down and fully encrypted. Because the search team managed to execute the court-authorized no-knock warrant in a timely manner, law enforcement agents seized the subject's computer while it was unencrypted. During the execution of a search

warrant on another user of "Website 19," the subject initiated the process of shutting down his computer and unplugged an encrypted drive before agents took him into custody. Some of his content was still open and decrypted but some was encrypted when he was detained. Because the agents executed the court-authorized no-knock warrant in a timely manner, crucial evidence was obtained and preserved. By contrast, during the execution of a search warrant on another user of "Website 19," the subject was not at his computer when agents entered the residence. His computers were shut down and fully encrypted. The subject's computers have not yet been decrypted.

56. Accordingly, in order to minimize the possibility that agents will encounter encrypted computers, your Affiant respectfully requests that this warrant be a "no knock" warrant allowing agents to make a dynamic entry into the residence before announcing their presence, in order to prevent the activation of encryption software, at any time of day or evening, at which agents can determine that the subject under investigation is home.

CONCLUSION

57. Based on the foregoing, there is probable cause to believe that the offenses described in ¶6 have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, including any detached buildings located on the property, authorizing the seizure and search of the items described in Attachment B.

58. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of the above mentioned crimes.

Sworn to under the pains and penalties of perjury.

Pamela S. Kirschner
Special Agent

Sworn to and subscribed before me this 15th day of October, 2014.

HON. KAREN L. LITKOVITZ
United States Magistrate Judge

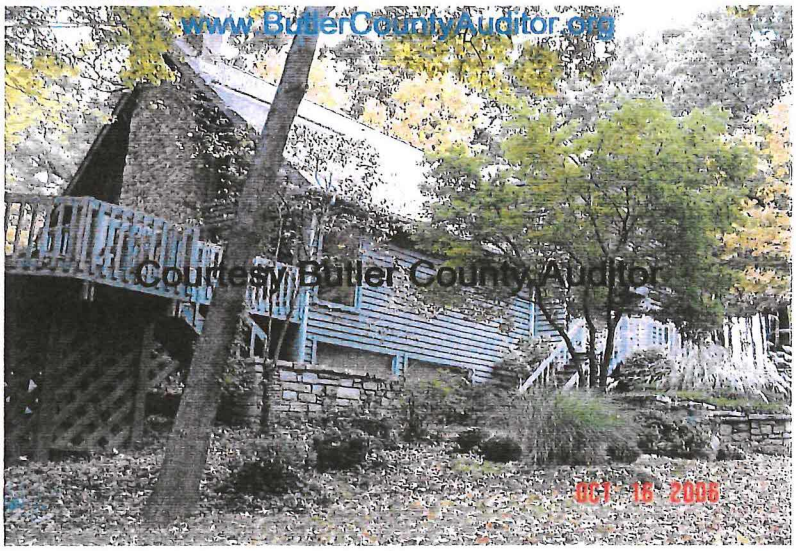
ATTACHMENT A

Place to be Searched

The residence located at 2000 Smith Road, Hamilton, Ohio 45013, is described as a one and a half to two-story frame and stone contemporary style single family residence. The residence is located in the middle of an approximately five acre wooded lot. There is a semi-circle shaped stone and concrete entrance façade with a black metal gate attached. A detached two-plus car garage and barn are also located near the residence.

View From Road (10/9/2014):

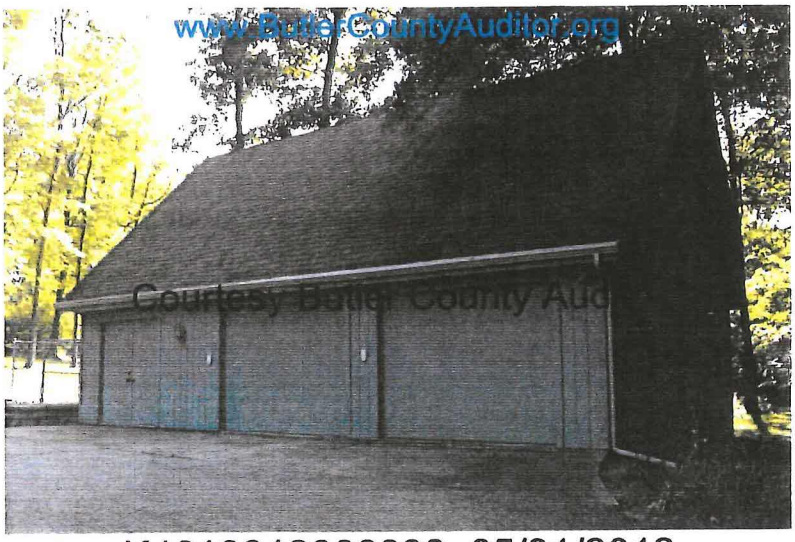
House Picture 1



House Picture 2

K4610012000039 05/31/2012

Garage



K4610012000039 05/31/2012

Land Overview with Entranceway Visible

ATTACHMENT B

Information to be Seized

1. Instrumentalities of the violations contained within the continuation for the search warrant at 2000 Smith Road, Hamilton, Ohio 45013:

a. any computer, computer system, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, hard drive and other computer related operation equipment, photographs and other visual depictions of such graphic interchange formats (JPG, GIF, TIF, AVI, and MPEG), electronic data storage devices (hardware, software, diskettes, backup tapes, CDs, DVD, flash memory devices, thumb drives, and other storage media); and any input/output peripheral devices, passwords, data security devices, and related security documentation;

b. books and magazines containing visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A);

c. originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A); and

d. motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in

which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

k. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet;

4. Any child pornography as defined by 18 U.S.C. § 2256(8);

5. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence;

6. Documents and records regarding the ownership and/or possession of the searched premises;

7. Credit card information, bills, and payment records;

8. Information or correspondence pertaining to affiliation with any child exploitation websites;

9. Any material that is "child erotica";

10. Any correspondence/records indicating the true identity of any member or user of "Website 19"; and

11. Any correspondence, e-mails, electronic messages, and records pertaining to "Website 19;"

As used above, the terms "records" and "information" refer to all forms of creation or storage, any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, videotapes, motion pictures, or photocopies).

The term "computer" refers to all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions: desktop computers, notebook computers, mobile phones, tablets, server computers, smart phones, and network hardware.

The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples are hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.